Съответствие на Curry-Howard

Трифон Трифонов

λ-смятане и теория на доказателствата, 2018/19 г.

21–28 май 2019 г.

Интерпретация на Brouwer-Heyting-Kolmogorov

В интуиционистката (конструктивната) логика можем да разглеждаме доказателствата като конструкции.

Доказателство на

1. $A \wedge B$ е комбинация от доказателства на A и B
2. $A \vee B$ е доказателство на A или на B с етикет a или b
3. $A \to B$ е конструкция, която по доказателство на A дава доказателство на B
4. $\forall_x A$ е конструкция, която по елемент x дава доказателство на $A(x)$
5. $\exists_x A$ е комбинация от елемент x и доказателство на $A(x)$

Формулите като типове

Можем да си мислим за формулите като за типове!

формула	тип
$A \to B$	$\rho \Rightarrow \sigma$
$A \wedge B$	$\rho \otimes \sigma$
$A \vee B$	$\rho \oplus \sigma$
съждителни променливи	типови променливи
$A[P \mapsto B]$	$\rho[\alpha \mapsto \sigma]$
атомарна формула $p\,x$	фамилия от базови типове $\{\mu_x\}$
$\forall_x A$	фамилия от типове $\{\rho_x\}$
$\exists_x A$	елемент на фамилия от типове ρ_x

Доказателствата като програми

Доказателство на формула като за типизиран терм

доказателство	λ-терм
$\dfrac{\begin{array}{c\|} M \end{array} \quad \begin{array}{c\|} N \end{array}}{A \to B \qquad A}\,{\to}^{-}$	апликация $(M^{A\to B}\, N^{A})^{B}$
$\dfrac{\begin{array}{c} [\cancel{A^{u}}] \\ \hline \vert\, M \end{array}}{B}\,{\to}^{+}\, u$	абстракция $(\lambda_{u^{A}} M^{B})^{A\to B}$
етикет u на допускане A	променлива u от тип A
задраскано допускане	свързана променлива
$\mathrm{FA}(M)$	$\mathrm{FV}(M)$
доказателство без свободни допускания	затворен терм
аксиома	константа

Доказателствата като програми (2)

доказателство	λ-терм
$\wedge^+ \dfrac{\begin{array}{cc} \mid M & \mid N \\ A & B \end{array}}{A \wedge B}$	наредена двойка $\langle M^A, N^B \rangle^{A \wedge B}$
$\wedge_0^- \dfrac{\begin{array}{c} \mid M \\ A \wedge B \end{array}}{A}$	лява проекция $(M^{A \wedge B} \llcorner)^A$
$\wedge_1^- \dfrac{\begin{array}{c} \mid M \\ A \wedge B \end{array}}{B}$	дясна проекция $(M^{A \wedge B} \lrcorner)^B$
разглеждане на случаи	разклонение (Cases)
индукция	рекурсия ($\mathcal{R}$)

Доказателствата като програми (3)

доказателство	λ-терм
$\forall^+ \dfrac{\begin{array}{c}\mid M \\ A\end{array}}{\forall_x A}\ x \notin FV[FA(M)]$	(зависима) абстракция $(\lambda_x M^A)^{\forall_x A}$
$\forall^- \dfrac{\begin{array}{cc}\mid M & \\ \forall_x A & t\end{array}}{A[x \mapsto t]}$	(зависима) апликация $(M^{\forall_x A}\, t)^{A[x \mapsto t]}$
$\exists^+ \dfrac{\begin{array}{cc} & \mid M \\ t & A[x \mapsto t]\end{array}}{\exists_x A}$	(зависима) наредена двойка $\left\langle t, M^{A[x \mapsto t]} \right\rangle^{\exists_x A}$

Програмите като доказателства

λ-терм		доказателство	
$\left((\lambda_{u^A} M^B)^{A\to B} N^A\right)^B$	(β-редекс)	$\dfrac{\dfrac{\dfrac{[\cancel{A^u}]}{\vert\ M}}{B}\ u}{A \to B} \to^+ \quad \vert\ N \qquad A \to^-$ B	(Cut)
$M^B[u^A \mapsto N^A]$	(β-редукт)	$\begin{array}{c} \vert\ N \\ [A] \\ \vert\ M \\ B \end{array}$	
β-редукция		елиминиране на Cut	
терм в нормална форма		доказателство без Cut	
теорема за силна нормализация		теорема за елиминиране на Cut	

Програмите като доказателства (2)

λ-терм	доказателство
$\left(\lambda_{u^A}\left(M^{A\to B}\,u^A\right)^B\right)^{A\to B} \xrightarrow{\eta} M^{A\to B}$	$\dfrac{\dfrac{\dfrac{\mid M}{A\to B} \quad \dfrac{}{\cancel{A}^{u}}}{B}\,{\to}^{+}}{A\to B}\,{\to}^{-} \xrightarrow{\eta} \dfrac{\mid M}{A\to B}\,u$
Λ^T	$Nm(\to)$
типова коректност	коректност на доказателство
обитаем тип	теорема
проверка за обитаемост	търсене на доказателство

HA^ω

Типове

$$\sigma, \tau \quad ::= \quad \alpha \mid \mathsf{B} \mid \mathsf{N} \mid \sigma \Rightarrow \tau \mid \sigma \otimes \tau$$

Термове

$$\begin{array}{rcll} s, t & ::= & x^\rho & \mid (\lambda_{x^\rho}\, t^\sigma)^{\rho \Rightarrow \sigma} \quad \mid (s^{\rho \Rightarrow \sigma}\, t^\rho)^\sigma \\ & & & \mid \mathsf{Pair}^{\rho \Rightarrow \sigma \Rightarrow \rho \otimes \sigma}_{\rho,\sigma} \quad \mid \mathsf{Split}_{\rho,\sigma,\tau} : \rho \otimes \sigma \Rightarrow (\rho \Rightarrow \sigma \Rightarrow \tau) \Rightarrow \tau \\ & & & \mid \mathsf{tt}^\mathsf{B} \mid \mathsf{ff}^\mathsf{B} \quad \mid \mathsf{Cases}_\tau : B \Rightarrow \tau \Rightarrow \tau \Rightarrow \tau \\ & & & \mid 0^\mathsf{N} \mid \mathsf{S}^{\mathsf{N} \Rightarrow \mathsf{N}} \quad \mid \mathcal{R}_\tau : \mathsf{N} \Rightarrow \tau \Rightarrow (\mathsf{N} \Rightarrow \tau \Rightarrow \tau) \Rightarrow \tau \end{array}$$

$$\langle s, t \rangle := \mathsf{Pair}\, s\, t, \quad t_\llcorner := \mathsf{Split}\, t\, (\lambda_{x,y} x), \quad t_\lrcorner := \mathsf{Split}\, t\, (\lambda_{x,y} y).$$

Редукции

$$\begin{array}{ll} (\lambda_x s)t \xrightarrow{\beta} s[x \mapsto t] & \mathsf{Split}\, \langle s, t \rangle\, f \xrightarrow{\beta} f\, s\, t \\ \mathsf{Cases}\, \mathsf{tt}\, s\, t \xrightarrow{\beta} s & \mathsf{Cases}\, \mathsf{ff}\, s\, t \xrightarrow{\beta} t \\ \mathcal{R}\, 0\, s\, t \xrightarrow{\beta} s & \mathcal{R}\, (\mathsf{S}n)\, s\, t \xrightarrow{\beta} t\, n\, (\mathcal{R}\, n\, s\, t) \end{array}$$

HA^ω

Формули

$$A, B \quad ::= \quad \mathrm{at}(t^{\mathsf{B}}) \mid A \to B \mid A \wedge B \mid A \vee B \mid \forall_{x^\rho} A \mid \exists_{x^\rho} A$$
$$F := \mathrm{at}(\mathrm{ff}^{\mathsf{B}}), \qquad T := \mathrm{at}(\mathrm{tt}^{\mathsf{B}}), \qquad \neg A := A \to F.$$

Доказателства

$$\begin{aligned} M, N \quad ::= \quad & u^A \mid \mathsf{AxT}^T \mid (\lambda_{u^A} M^B)^{A\to B} \mid (M^{A\to B} N^A)^B \\ & \mid \wedge^+_{A,B} : A \to B \to A \wedge B \\ & \mid \wedge^-_{A,B,C} : A \wedge B \to (A \to B \to C) \to C \\ & \mid \vee^{+0}_{A,B} : A \to A \vee B \mid \vee^{+1}_{A,B} : B \to A \vee B \\ & \mid \vee^-{}_{A,B,C} : A \vee B \to (A \to C) \to (B \to C) \to C \\ & \mid (\lambda_{x^\rho} M^A)^{\forall_{x^\rho} A} \quad (x \notin \mathsf{FV}[\mathsf{FA}(M)]) \mid (M^{\forall_{x^\rho} A} t^\rho)^{A[x\mapsto t]} \\ & \mid \exists^+_{x,A} : \forall_{x^\rho}(A \to \exists_{x^\rho} A) \\ & \mid \exists^-_{x,A,C} : \exists_{x^\rho} A \to \forall_{x^\rho}(A \to C) \to C \quad (x \notin \mathsf{FV}(C)) \\ & \mid \mathcal{C}_{b,A} : \forall_{b^{\mathbf{B}}}(A[b \mapsto \mathrm{tt}] \to A[b \mapsto \mathrm{ff}] \to A) \\ & \mid \mathsf{Ind}_{n,A} : \forall_{n^{\mathbf{N}}}(A[n \mapsto 0] \to \forall_n(A \to A[n \mapsto \mathsf{S}\, n]) \to A) \end{aligned}$$